SPYWOLF

Security Audit Report

Completed on
June 15, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **RemeDao** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

"

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

– SPYWOLF Team –

"

TABLE OF CONTENTS

SPYWOLF.CO

RemeDao

PROJECT DESCRIPTION

According to their whitepaper:

The RemeDAO will be rebase token system which will pay holders compounded rewards Everyday. In the DAO, users can propose and vote for their favorite meme tokens. The most vote token will be bought and distributed automatically by the RemeDAO system right after the voting end.

Release Date: June 14, 2022
Category: Rebase/DAO

01

CONTRACT INFO

Token Name
Remedao

Symbol
RMD

Contract Address
0x577d0b05FaFA1b320EB30808E34a3e199C1bdA92

Network
Binance Smart Chain

Language
Solidity

Deployment Date
July 14, 2022

Verified?
Yes

Total Supply
1,500,000

Status
Not launched

TAXES

Buy Tax
10%

Sell Tax
10%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

02

CURRENT STATS

(As of June 15, 2022)

Status:
Not Launched

Liquidity

Not added yet
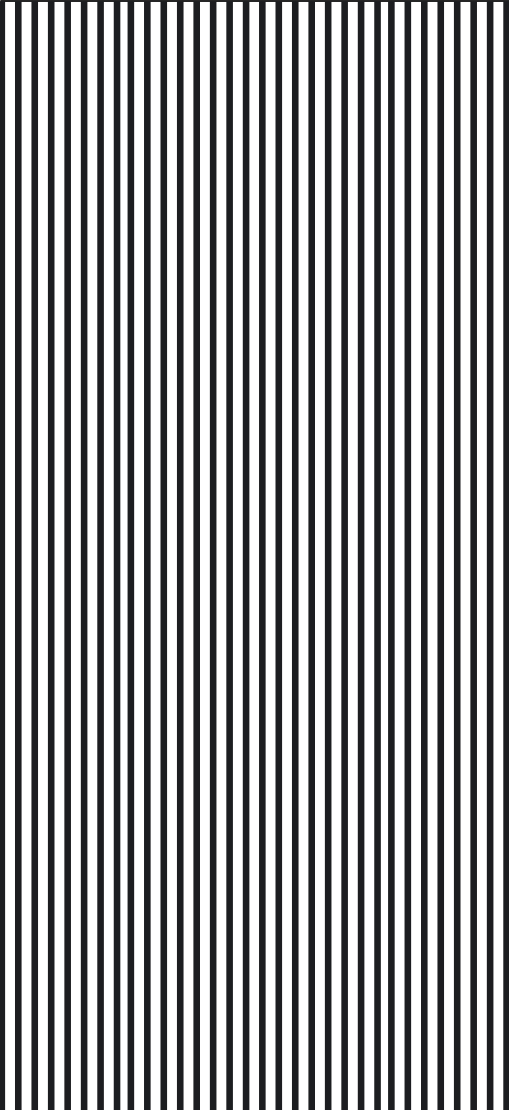
Burn

No burnt tokens

MaxTxAmount

10% of holder's balance

Additional Info

Rebase token with changing supply

LP Address(es)

Liquidity not added yet

03

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	1500000 RMD
Median Transfer Amount	1500000 RMD
Average Transfer Amount	1500000 RMD
First transfer date	2022-06-14
Last transfer date	2022-06-14
Days token transferred	1

SMART CONTRACT STATS

Calls Count	2
External calls	2
Internal calls	0
Transactions count	2
Uniq Callers	1
Days contract called	1
Last transaction time	2022-06-14 10:12:18 UTC
Created	2022-06-14 10:09:24 UTC
Create TX	0xdff629beb13d4724b6b1d05d7273dfdec2df47f822fa19f2f15fb16180a6f7e2
Creator	0x7777074a1f955631cbeda52f2900d6cc3ce29999

FEATURED WALLETS

Owner address	0x7777074a1f955631cbeda52f2900d6cc3ce29999
Treasury receiver	0x0000a9fdb9d4f7949d5b8060e4e93c7107729999
Insurance fund receiver	0x4444d2a65d1f75f56f8b9d3f4d3fe55631bd6666
Vote contract	0x4934df96683cbd46f1ab88b53e2dccb6d893442c
LP address	**Liquidity not added yet**

TOP 3 UNLOCKED WALLETS

1

100%   Same as treasury receiver

05
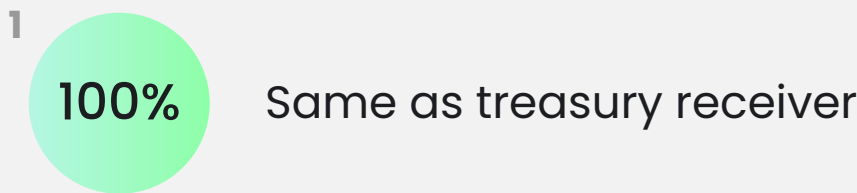
VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠️ High Risk

Owner can set lockAddress to any address once.
Along with total supply increasing with each rebase, the
lockAddress' balances are increased too if its holdings are above
500,000 and if it is not the zero address (0x00000000000000000000).

```solidity
uint256 lockMaxBalance = 5 * 10**5 * 10**DECIMALS;

function setLockAddress(address _address) external onlyOwner {
        require(lockAddress == address(0));
        lockAddress = _address;
}


function rebase() internal {
........................
_totalSupply = _totalSupply
    .mul(((10**RATE_DECIMALS).add(rebaseRate))**times)
    .div((10**RATE_DECIMALS)**times);

gonsPerFragment = TOTAL_GONS.div(_totalSupply);
pairContract.sync();
_rebaseEpoch = epoch;
if (lockAddress != address(0)) {
    if (balanceOf(lockAddress) > lockMaxBalance) {
        _gonBalances[lockAddress] = lockMaxBalance.mul(gonsPerFragment);
        _gonBalances[offChainGameReceiver] = _gonBalances[
            offChainGameReceiver
        ].add(
                _gonBalances[lockAddress] -
                    lockMaxBalance.mul(gonsPerFragment)
            );
        _updateAccountSnapshot(lockAddress);
        _updateAccountSnapshot(offChainGameReceiver);
    }
}
emit Rebase(epoch, _totalSupply);
}
```

08-

FOUND THREATS

⚠️ Medium Risk

This is rebase token with increasing supply up to uint256 (1 with 255 zeroes). Current supply is 1,500,000.
This can lead to token price inflation in future.

Once started by the owner, rebasing cannot be stopped.

```solidity
function startRebase() external onlyOwner {
    require(!isStartRebase);
    isStartRebase = true;
    _autoRebase = true;
    _rebaseStartTime = block.timestamp;
}

function shouldRebase() internal view returns (bool) {
    uint256 epoch = currentRebaseEpoch();
    return
        isStartRebase &&
        _autoRebase &&
        msg.sender != pair &&
        !inSwap &&
        epoch > _rebaseEpoch;
}
```

If holder is represented in the vote contract, he will be unable to sell.

```solidity
function _transferFrom(address sender,address recipient,uint256 amount
) internal returns (bool) {
.....................
if (address(voteContract) != address(0)) {
    require(!voteContract.lockVote(epoch, sender));
}
.....................
}
```

FOUND THREATS

⚠️ Medium Risk

Owner can change max sell transaction limit per epoch, based on percentage of holder's balance. Max sell tx can't be set lower than 5% of holder's balance.

```solidity
uint256 lockMaxBalance = 5 * 10**5 * 10**DECIMALS;

function setLockAddress(address _address) external onlyOwner {
        require(lockAddress == address(0));
        lockAddress = _address;
}

function rebase() internal {
........................
_totalSupply = _totalSupply
    .mul(((10**RATE_DECIMALS).add(rebaseRate))**times)
    .div((10**RATE_DECIMALS)**times);

gonsPerFragment = TOTAL_GONS.div(_totalSupply);
pairContract.sync();
_rebaseEpoch = epoch;
if (lockAddress != address(0)) {
    if (balanceOf(lockAddress) > lockMaxBalance) {
        _gonBalances[lockAddress] = lockMaxBalance.mul(gonsPerFragment);
        _gonBalances[offChainGameReceiver] = _gonBalances[
            offChainGameReceiver
        ].add(
                _gonBalances[lockAddress] -
                    lockMaxBalance.mul(gonsPerFragment)
            );
        _updateAccountSnapshot(lockAddress);
        _updateAccountSnapshot(offChainGameReceiver);
    }
}
emit Rebase(epoch, _totalSupply);
}
```

08-

FOUND THREATS

⚠️ Low Risk

Owner can set buy/sell fees up to 12% (combined buy+sell=24%).

```
function setFee(
    uint256 _treasuryFee,
    uint256 _insuranceFundFee,
    uint256 _memeFee
) external onlyOwner {
    require(_treasuryFee + _insuranceFundFee + _memeFee < 120);
    treasuryFee = _treasuryFee;
    insuranceFundFee = _insuranceFundFee;
    memeFee = _memeFee;
    totalFee = treasuryFee.add(insuranceFundFee).add(memeFee);
}
```

GOOD PRACTICES

RemeDAO
GOOD PRACTICES FOUND

1. Consider fundamental tradeoffs

2. Be attentive to blockchain properties

3. Ensure careful rollouts

4. Keep contracts simple

5. Stay up to date and track development

- ✔ The owner cannot mint new tokens after deployment

- ✔ The owner cannot stop or pause the contract

- ✔ The smart contract utilizes "SafeMath" to prevent overflows

- ✔ The owner cannot set fees above reasonable levels.

*⚠️ There is no information about tokens distribution based on the project's whitepaper and/or website.

TOKENOMICS

THE TEAM

The team at **RemeDao** has privately doxxed to SPYWOLF by completing the following KYC requirements:

- ID Verification
- Video statement
- Video interview with devs
- Owner's wallet verification

KYC INFORMATION

Issuer

SPYWOLF

Members

KYC Date

June 13, 2022

Format

Image

Certificate Link

https://github.com/SpyWolfNetwork/KYCs/blob/main/june/KYC_RemeDAO_0x577d0b05FaFA1b320EB30808E34a3e199C1bdA92.png

SpyWolf

KYC CERTIFICATE

This is to certify that

RemeDAO

0x577d0b05FaFA1b320EB30808E34a3e199C1bdA92

Has passed the KYC verification process on

June 15, 2022

SpyWolf.Network

ALWAYS REVIEW AUDIT BEFORE INVESTING

KYC CERTIFICATE · VERIFIED BY SPYWOLF

11

Website URL
https://remedao.com/

Domain Registry
https://www.namesilo.com/

Domain Expiration
Expires on 2023-06-12

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design, appropriate color scheme.

Content
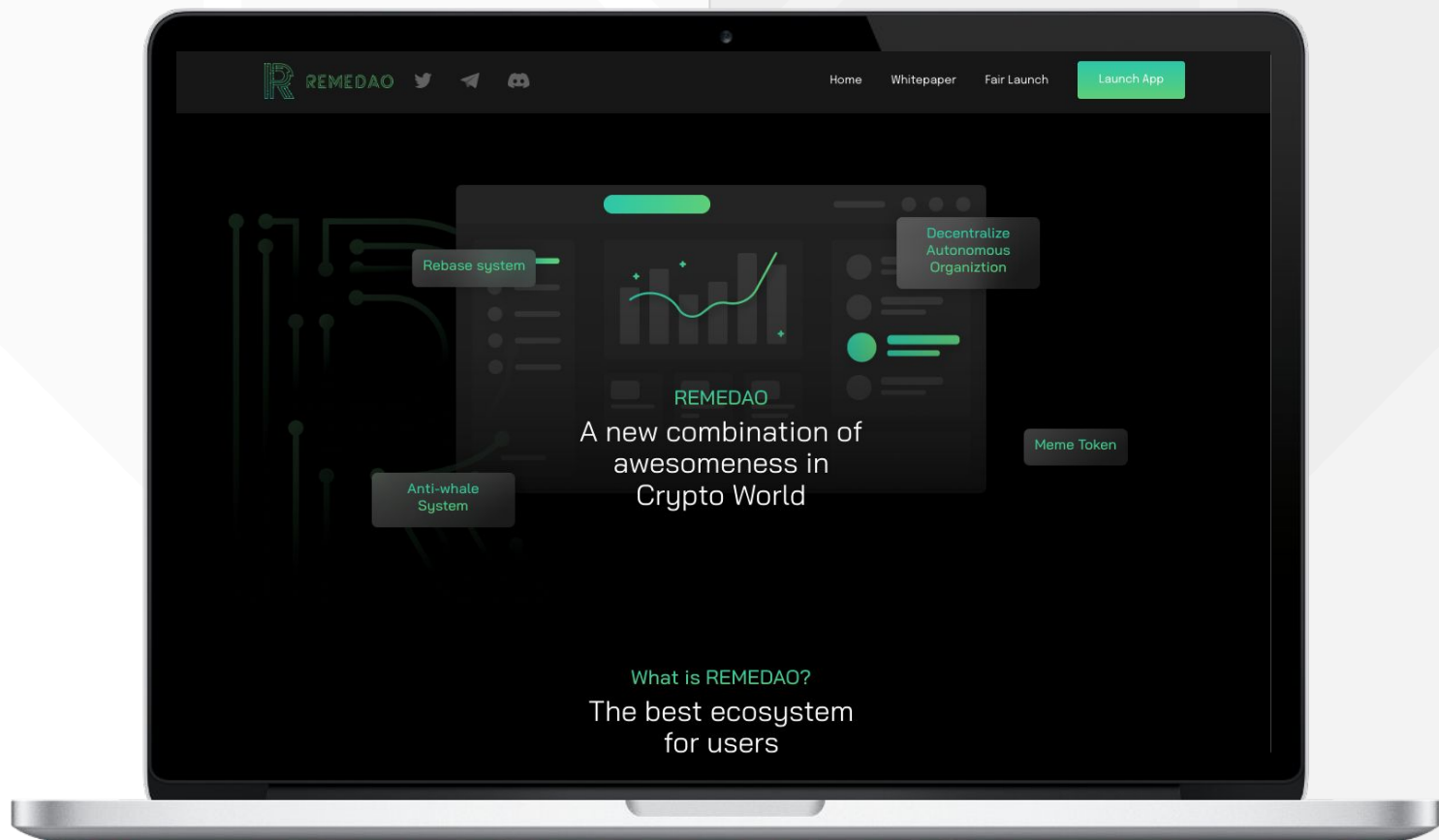Informational, no grammar mistakes.

Whitepaper
No whitepaper present. ⚠️

Roadmap
No roadmap present. ⚠️

Mobile-friendly?
Yes

REMEDAO • Home • Whitepaper • Fair Launch • Launch App

Rebase system

Decentralize Autonomous Organiztion

REMEDAO
A new combination of awesomeness in Crypto World

Anti-whale System

Meme Token

What is REMEDAO?
The best ecosystem for users

remedao.com

12

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS
The project's social media presence is very new and inactive.

Twitter

https://twitter.com/RemeDAOBSC
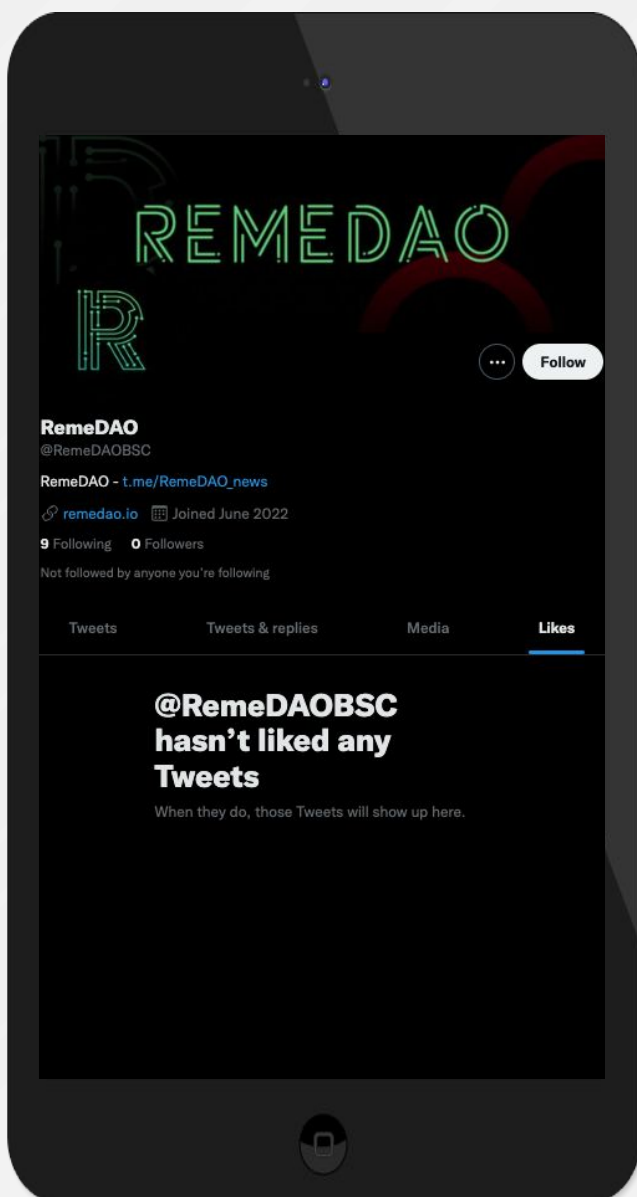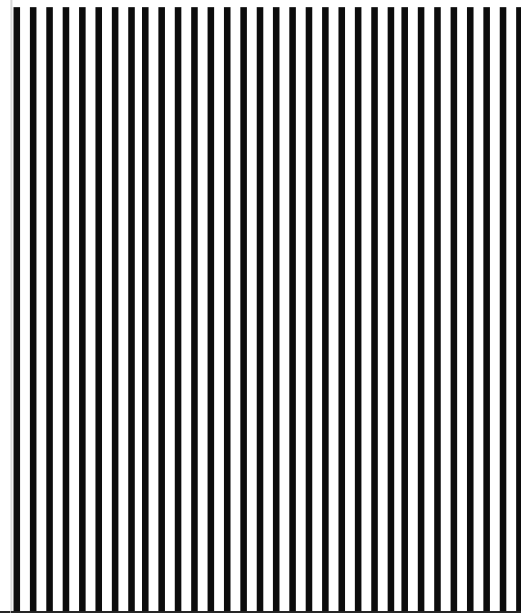
- 2 702 Followers, botted ⚠️
- Not active, 2 posts ⚠️

Discord

- Not available

Telegram

https://t.me/RemeDAO_news

- 6 728 members botted ⚠️
- Announcement channel

Medium

- Not available

13

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✔ **OVER 150 SUCCESSFUL CLIENTS**
- ✔ **MORE THAN 500 SCAMS EXPOSED**
- ✔ **MILLIONS SAVED IN POTENTIAL FRAUD**
- ✔ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- ✔ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to contact@spywolf.co or t.me/joe_SpyWolf

FIND US ONLINE

🌐 SPYWOLF.CO

🌐 SPYWOLF.NETWORK

✈ @SPYWOLFNETWORK

✈ @SPYWOLFOFFICIAL

🐦 @SPYWOLFNETWORK

🐙 @SPYWOLFNETWORK

14

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.